the individual clearly understands how the compromise occurred.

(iii) The individual shall be informed of what protective actions the Component is taking or the individual can take to mitigate against potential future harm. The Component should refer the individual to the Federal Trade Commission's public Web site on identity theft at *http://www.consumer.gov/idtheft/con_steps.htm.* The site provides valuable information as to what steps individuals can take to protect themselves if their identities potentially have been or are stolen.

(iv) A sample notification letter is at appendix B.

(b) The notification shall be made whether or not the personal information is contained in a system of records (See § 310.10(a)).

Subpart C—Collecting Personal Information

§ 310.15 General considerations.

(a) *Collect directly from the individual.* Collect to the greatest extent practicable personal information directly from the individual to whom it pertains if the information may result in adverse determination about an individual's rights, privileges, or benefits under any Federal program.

(b) *Collecting social security numbers (SSNs).* (1) It is unlawful for any Federal, State, or local governmental agency to deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide his or her SSN. However, if a Federal statute requires the SSN be furnished or if the SSN is furnished to a DoD Component maintaining a system of records in existence that was established and in operation before January 1, 1975, and the SSN was required under a statute or regulation adopted prior to this date for purposes of verifying the identity of an individual, this restriction does not apply.

(2) When an individual is requested to provide his or her SSN, he or she must be told:

(i) What uses will be made of the SSN;

(ii) The statute, regulation, or rule authorizing the solicitation of the SSN; and

(iii) Whether providing the SSN is voluntary or mandatory.

(3) Include in any systems notice for any system of records that contains SSNs a statement indicating the authority for maintaining the SSN.

(4) E.O. 9397,''Numbering System for Federal Accounts Relating to Individual Persons'', November 30, 1943, authorizes solicitation and use of SSNs as a numerical identifier for Federal personnel that are identified in most Federal record systems. However, it does not constitute authority for mandatory disclosure of the SSN.

(5) Upon entrance into military service or civilian employment with the Department of Defense, individuals are asked to provide their SSNs. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records. The notification in paragraph (b)(2) of this section shall be provided the individual when originally soliciting his or her SSN. The notification is not required if an individual is requested to furnish his SSN for identification purposes and the SSN is solely used to verify the SSN that is contained in the records. However, if the SSN is solicited and retained for any purposes other than verifying the existing SSN in the records, the requesting official shall provide the individual the notification required by paragraph (b)(2) of this section.

(6) Components shall ensure that the SSN is only collected when there is a demonstrated need for collection. If collection is not essential for the purposes for which the record or records are being maintained, it should not be solicited.

(7) DoD Components shall continually review their use of the SSN to determine whether such use can be eliminated, restricted, or concealed in Component business processes, systems and paper and electronic forms. While use of the SSN may be essential for program integrity and national security when information about an individual is disclosed outside the DoD, it may not be as critical when the information is being used for internal Departmental purposes.

(c) *Collecting personal information from third parties.* When information being solicited is of an objective nature and is not subject to being altered, the information should first be collected from the individual. But it may not be practicable to collect personal information first from the individual in all cases. Some examples of this are:

(1) Verification of information through third-party sources for security or employment suitability determinations;

(2) Seeking third-party opinions such as supervisor comments as to job knowledge, duty performance, or other opinion-type evaluations;

(3) When obtaining information first from the individual may impede rather than advance an investigative inquiry into the actions of the individual; and

(4) Contacting a third party at the request of the individual to furnish certain information such as exact periods of employment, termination dates, copies of records, or similar information.

(d) *Privacy Act Statements.* (1) When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a Privacy Act Statement is required regardless of the medium used to collect the information (forms, personal interviews, telephonic interviews, or other methods). The Privacy Act Statement consists of the elements set forth in paragraph (d)(2)of this section. The statement enables the individual to make an informed decision whether to provide the information requested. If the personal information solicited is not to be incorporated into a system of records, the statement need not be given. However, personal information obtained without a Privacy Act Statement shall not be incorporated into any system of records. When soliciting SSNs for any purpose, see paragraph (b)(2) of this section.

(2) The Privacy Act Statement shall include:

(i) The Federal statute or Executive Order that authorizes collection of the requested information (See § 310.10(d)).

(ii) The principal purpose or purposes for which the information is to be used;

(iii) The routine uses that will be made of the information (See § 310.22(d));

(iv) Whether providing the information is voluntary or mandatory (See paragraph (e) of this section); and

(v) The effects on the individual if he or she chooses not to provide the requested information.

(3) The Privacy Act Statement shall be concise, current, and easily understood.

(4) The Privacy Act statement may appear as a public notice (sign or poster), conspicuously displayed in the area where the information is collected, such as at check-cashing facilities or identification photograph facilities (but see § 310.16(a)).

(5) The individual normally is not required to sign the Privacy Act Statement.

(6) The individual shall be provided a written copy of the Privacy Act Statement upon request. This must be done regardless of the method chosen to furnish the initial advisement.

(e) *Mandatory as opposed to voluntary disclosures.* Include in the Privacy Act Statement specifically whether furnishing the requested personal data is mandatory or voluntary. A requirement to furnish personal data is mandatory only when the DoD Component is authorized to impose a penalty on the individual for failure to provide the requested information. If a penalty cannot be imposed, disclosing the information is always voluntary.

§ 310.16 Forms.

(a) *DoD Forms.* (1) DoD Instruction 7750.7[8] provides guidance for preparing Privacy Act Statements for use with forms (see also paragraph (b) of this section).

(2) When forms are used to collect personal information, the Privacy Act Statement shall appear as follows (listed in the order of preference):

(i) In the body of the form, preferably just below the title so that the reader will be advised of the contents of the statement before he or she begins to complete the form;

[8] See footnote 1 to § 310.1.